

<http://www19.ipdl.ncipi.go.jp/PA1/result/detail/main/wAAApLaWW4DA406152587...> 2005/01/05

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

8

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平6-152587

(43)公開日 平成6年(1994)5月31日

(51)Int.Cl. ⁵	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/06 9/14		7117-5K	H 0 4 L 9/ 02	Z

審査請求 未請求 請求項の数3(全 6 頁)

(21)出願番号 特願平4-295766
(22)出願日 平成4年(1992)11月5日

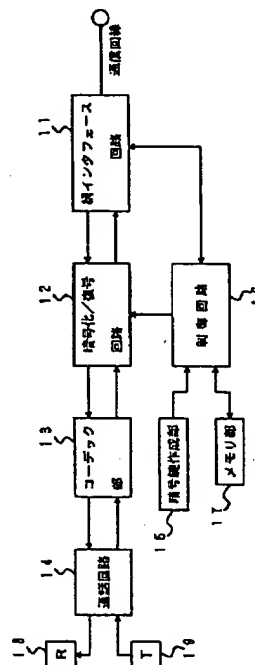
(71)出願人 000004226
日本電信電話株式会社
東京都千代田区内幸町一丁目1番6号
(72)発明者 松沢 裕之
東京都千代田区内幸町1丁目1番6号 日
本電信電話株式会社内
(72)発明者 壁谷 喜義
東京都千代田区内幸町1丁目1番6号 日
本電信電話株式会社内
(74)代理人 弁理士 吉田 精孝

(54)【発明の名称】 デジタル通信方法及びその装置

(57)【要約】

【目的】 通信端末同士で通信毎に通信用暗号鍵を変更可能なデジタル通信方法及びその装置を提供する。

【構成】 通信の開始時に、暗号鍵作成部15により通信用暗号鍵を自動的に生成し、これをメモリ部17に記憶された通信用暗号鍵解読鍵を用いて暗号化/復号回路12により暗号化し、これを網インタフェース回路11を通して受信側へ送信し、受信側では、該受信した前記暗号化された通信用暗号鍵を前記通信用暗号鍵解読鍵を用いて暗号化/復号回路12により復号化し、以後、該通信用暗号鍵を用いてデジタル情報を暗号化及び復号して通信する。



【特許請求の範囲】

【請求項1】 秘密鍵暗号方式によりデジタル情報を暗号化して伝送するデジタル通信方法において、送信側では、通信の開始時に通信用暗号鍵を自動的に作成し、該通信用暗号鍵を通信用暗号鍵読鍵を用いて暗号化し、該暗号化した通信用暗号鍵を他のデジタル情報に先だって送信し、受信側では、暗号化された通信用暗号鍵を前記通信用暗号鍵読鍵を用いて復号し、以後、該通信用暗号鍵を用いてデジタル情報を暗号化及び復号して通信するようになったことを特徴とするデジタル通信方法。

【請求項2】 秘密鍵暗号方式によりデジタル情報を暗号化して送信するデジタル通信装置において、通信用暗号鍵を暗号化するための通信用暗号鍵読鍵を記憶する記憶手段と、通信の開始時に通信用暗号鍵を自動的に作成する通信用暗号鍵作成手段と、前記通信用暗号鍵を前記通信用暗号鍵読鍵を用いて暗号化する通信用暗号鍵暗号化手段と、該暗号化した通信用暗号鍵を他のデジタル情報に先だって送信する送信手段とを備えたことを特徴とするデジタル通信装置。

【請求項3】 秘密鍵暗号方式により暗号化されたデジタル情報を受信するデジタル通信装置において、通信用暗号鍵を復号するための通信用暗号鍵読鍵を記憶する記憶手段と、暗号化された通信用暗号鍵を受信する受信手段と、該受信した暗号化された通信用暗号鍵を前記通信用暗号鍵読鍵を用いて復号する通信用暗号鍵復号手段とを備えたことを特徴とするデジタル通信装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、テキスト、音声、画像データ等のデジタル情報を暗号化して伝送するデジタル通信方法及びその装置に関するものである。

【0002】

【従来の技術】 従来より、この種の通信方法に使用される暗号方式は種々提案されているが、そのうち1つに秘密鍵暗号方式と呼ばれるものがある。この方式は送信時に任意の秘密の情報（暗号鍵）を用いて暗号化するとともに、受信時に同一の暗号鍵を用いて復号する方式である。秘密鍵暗号方式の暗号化及び復号のアルゴリズムとしては、FEAL（Fast Data Encipherment Algorithm: 高速データ暗号アルゴリズム）やDES（Data Encryption Standard: 米国連邦規格の暗号アルゴリズム）等が知られており、これらのアルゴリズム又はアルゴリズム

を組込んだLSIを用いることにより、容易に暗号化及び復号を行うことができる。

【0003】 前述した秘密鍵暗号方式を用いた従来の通信方法として、センタにより暗号鍵を集中的に管理して通信する方法がある。図2は前述した従来の通信方法による通信のようすを示すもので、図中、1は鍵管理センタ、2は発信端末、3は着信端末である。鍵管理センタ1には、暗号通信を行う端末の各ID及びこれに対応する通信用暗号鍵読鍵を予め登録しておくものとする。

10 【0004】 発信端末2は発信時に鍵管理センタ1へ自分のID#i及び着信先のID#jを送り、通信用暗号鍵Ksを要求する(I)。鍵管理センタ1は発信側のID#i及び着信側のID#jより両端末の通信用暗号鍵読鍵Ki、Kjを検索するとともに、通信用暗号鍵Ksを自動的に作成する。次に、鍵管理センタ1は発信側のID#i及び通信用暗号鍵Ksを通信用暗号鍵読鍵Kjで暗号化し、得られたEij(Ks, #i)に通信用暗号鍵Ks及び着信側のID#jを加え、さらに通信用暗号鍵読鍵Kiで暗号化し、得られたEij(Ks, #j, Eij(Ks, #i))を発信端末2に送る(II)。

【0005】 発信端末2は送られてきた情報を通信用暗号鍵読鍵Kiで復号し、得られたKsを通信時の暗号鍵として使用するとともに、Eij(Ks, #i)をそのまま着信端末3に送る(III)。着信端末3では送られてきた情報を通信用暗号鍵読鍵Kjで復号し、得られた通信用暗号鍵Ks、即ち発信端末2側と同一の暗号鍵により暗号通信を行う(IV)。

【0006】

30 【発明が解決しようとする課題】 しかしながら、前記方法では鍵管理センタが必要となり、また、発信側は着信側との通信に先立って該鍵管理センタに通信用暗号鍵を要求しなければならず、複雑な操作が必要となる等の問題があった。

【0007】 本発明は前記従来の問題点に鑑み、通信端末同士で通信毎に通信用暗号鍵を変更可能なデジタル通信方法及びその装置を提供することを目的とする。

【0008】

40 【課題を解決するための手段】 前記目的を達成するため、本発明の請求項1では、秘密鍵暗号方式によりデジタル情報を暗号化して伝送するデジタル通信方法において、送信側では、通信の開始時に通信用暗号鍵を自動的に作成し、該通信用暗号鍵を通信用暗号鍵読鍵を用いて暗号化し、該暗号化した通信用暗号鍵を他のデジタル情報に先だって送信し、受信側では、暗号化された通信用暗号鍵を前記通信用暗号鍵読鍵を用いて復号し、以後、該通信用暗号鍵を用いてデジタル情報を暗号化及び復号して通信するようになったデジタル通信方法を提案する。

50 【0009】 また、請求項2では、秘密鍵暗号方式によりデジタル情報を暗号化して送信するデジタル通信

装置において、通信用暗号鍵を暗号化するための通信用暗号鍵解読鍵を記憶する記憶手段と、通信の開始時に通信用暗号鍵を自動的に作成する通信用暗号鍵作成手段と、前記通信用暗号鍵を前記通信用暗号鍵解読鍵を用いて暗号化する通信用暗号鍵暗号化手段と、該暗号化した通信用暗号鍵を他のデジタル情報に先だって送信する送信手段とを備えたデジタル通信装置を提案する。

【0010】また、請求項3では、秘密鍵暗号方式により暗号化されたデジタル情報を受信するデジタル通信装置において、通信用暗号鍵を復号するための通信用暗号鍵解読鍵を記憶する記憶手段と、暗号化された通信用暗号鍵を受信する受信手段と、該受信した暗号化された通信用暗号鍵を前記通信用暗号鍵解読鍵を用いて復号する通信用暗号鍵復号手段とを備えたデジタル通信装置を提案する。

【0011】

【作用】本発明の請求項1によれば、通信の開始時に、送信側において通信用暗号鍵が自動的に作成され、これが通信用暗号鍵解読鍵によって暗号化された上で他の情報に先だって受信側へ送信され、受信側ではこれが送信側と同一の通信用暗号鍵解読鍵によって復号され、以後、この通信用暗号鍵による暗号通信がなされる。

【0012】また、請求項2によれば、通信の開始時に、通信用暗号鍵作成手段により通信用暗号鍵が自動的に作成され、通信用暗号鍵暗号化手段により予め記憶手段に記憶された通信用暗号鍵解読鍵を用いて暗号化され、送信手段により他の情報に先だって受信側へ送信される。

【0013】また、請求項3によれば、受信手段により暗号化された通信用暗号鍵が受信され、これが通信用暗号鍵復号手段により予め記憶手段に記憶された通信用暗号鍵解読鍵を用いて復号される。

【0014】

【実施例】図1は本発明のデジタル通信装置の一実施例を示すもので、ここでは通話を主目的としたものを示す。図中、11は送信情報を通信回線に対応した信号に変換して送信したり、通信回線を介して送られてくる信号を受信情報に変換したり、発信や着信のための制御信号を送信又は受信するための網インタフェース回路、12は汎用のCPU及びROM、RAM等又は専用のLSIで構成され、暗号鍵を用いて送信情報の暗号化及び受信信号の復号を行うための暗号化／復号回路、13はデジタル信号をアナログ信号に変換したり、アナログ信号をデジタル信号に変換するコーデック部、14は送話器から入力された信号や受話器へ出力する信号を増幅する通話回路、15は各通信毎に異なる通信用暗号鍵を自動的にランダムに作成する暗号鍵作成部、16は汎用のCPU及びROM、RAM等で構成され、各部を制御する制御回路、17は通信用暗号鍵を暗号化又は復号する際に使用する通信用暗号鍵解読鍵を記憶するメモ

リ部、18は受話器、19は送話器である。なお、通信用暗号鍵解読鍵を記憶するためのメモリ部17は容量が少なく済むので、独立したメモリ部17を設ける代わりに制御回路16を構成するメモリの空き空間を使用することも可能である。

【0015】図3及び図4は発信時及び着信時の動作を示すフローチャートであり、以下、これらに従って本装置の動作を説明する。

【0016】最初に、発信時の動作を説明する。まず、装置に対してオフフック・ダイヤル押下等により発信操作をする（ステップS1）と、制御回路16は通信用暗号鍵解読鍵をメモリ部17から読み出し、暗号化／復号回路12に書き込み（ステップS2）、網インタフェース回路11に発信の指示を行う（ステップS3）。着信側の装置が応答し、通話回路14が接続される（ステップS4）と、制御回路16は通信用暗号鍵の作成を暗号鍵作成部15に指示する（ステップS5）。次に、暗号鍵作成部15で自動的に作成した通信用暗号鍵を暗号化／復号回路12において通信用暗号鍵解読鍵を用いて暗号化し（ステップS6）、該暗号化した通信用暗号鍵を網インタフェース回路11を通して通信回線に送出し（ステップS7）、通話を開始する（ステップS8）。

【0017】送話器19から入力された送話信号は通話回路14で増幅され、コーデック部13でデジタル信号に変換された後、暗号化／復号回路12において制御回路16から書き込まれた通信用暗号鍵を用いて暗号化された後、網インタフェース回路11を通して通信回線に送出される。一方、網インタフェース回路11を通して通信回線から受信した受信信号は、暗号化／復号回路12において制御回路16から書き込まれた通信用暗号鍵を用いて復号された後、コーデック部13でアナログ信号に変換され、通話回路14で増幅され、受話器18から受話信号として出力される。

【0018】なお、暗号鍵作成部15で作成する通信用暗号鍵の作成方法は、各種ランダム関数により乱数を発生させる方法、日付け・時間等を初期値にして一定のアルゴリズムで生成させる方法等がある。また、メモリ部17に記憶する通信用暗号鍵解読鍵としては通信相手毎に異なるものとしても良く、要は発信側及び受信側で同一のものを誤りなく使用できれば良い。また、図3において、通信用暗号鍵解読鍵書き込み処理（ステップS2）は、通話回路接続処理（ステップS4）の直後に行っても同一の結果が得られる。

【0019】次に、着信時の動作を説明する。通信回線から着信がある（ステップSP1）と、制御回路16は通信用暗号鍵解読鍵をメモリ部17から読み出し、暗号化／復号回路12に書き込む（ステップSP2）。オフフック等により着信操作を行って（ステップSP3）、通話回路14が接続された（ステップSP4）後、網インタフェース回路11を通して通信回線から通信用暗号

鍵解読鍵によって暗号化された通信用暗号鍵を受信する（ステップSP5）と、暗号化／復号回路12で通信用暗号鍵解読鍵を用いて復号し（ステップSP6）、該復号した通信用暗号鍵を暗号化／復号回路12に書き込む（ステップSP7）。そして、通信が開始された後は、前述した発信時の場合と同様に通信を行う（ステップSP8）。なお、図4において、通信用暗号鍵解読鍵書き込み処理（ステップSP2）は、通話回路接続処理（ステップSP4）の直後に行っても同一の結果が得られる。

【0020】図5は本発明のデジタル通信装置の他の実施例を示すもので、ここではデータ通信を主目的としたものを示す。即ち、図1の実施例において、コーデック部13及び通話回路14を、それぞれデータ入出力インタフェース回路21及びデータ入出力装置22に置き換えたものである。データ入出力装置22から入力された送信データはデータ入出力インタフェース回路21を通り、暗号化／復号回路12において制御回路16から書き込まれた通信用暗号鍵を用いて暗号化された後、網インタフェース回路11を通して通信回線に送出される。一方、網インタフェース回路11を通して通信回線から受信した受信信号は、暗号化／復号回路12において制御回路16から書き込まれた通信用暗号鍵を用いて復号化された後、データ入出力インタフェース回路21を通り、データ入出力装置22から受信データとして出力される。なお、その他の構成及び動作は図1の実施例と同様である。

*【0021】

【発明の効果】以上説明したように本発明によれば、送信側において通信毎に自動的に通信用暗号鍵を作成し、これを受信側で誤りなく解読することができる、即ち通信用暗号鍵の作成のための鍵管理センタを必要とすることなく、当事者間で通信用暗号鍵を各通信毎に変更することができる、これによって複雑な操作を要することなく、通信の開始時（暗号鍵の送信時）を除いて第三者からの盗聴を困難とすることができ、通信のセキュリティを向上させることができる利点がある。

【図面の簡単な説明】

【図1】本発明のデジタル通信装置の一実施例を示す構成図

【図2】従来の秘密鍵暗号方式を用いた通信方法の説明図

【図3】本発明装置の発信時の動作を示すフローチャート

【図4】本発明装置の着信時の動作を示すフローチャート

【図5】本発明のデジタル通信装置の他の実施例を示す構成図

【符号の説明】

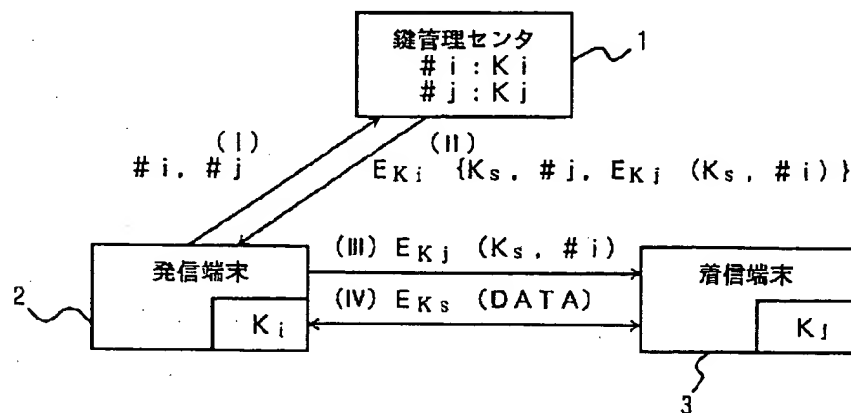
11…網インタフェース回路、12…暗号化／復号回路、13…コーデック部、14…通話回路、15…暗号鍵作成部、16…制御回路、17…メモリ部、18…受話器、19…送話器、21…データ入出力インタフェース回路、22…データ入出力装置。

【図2】

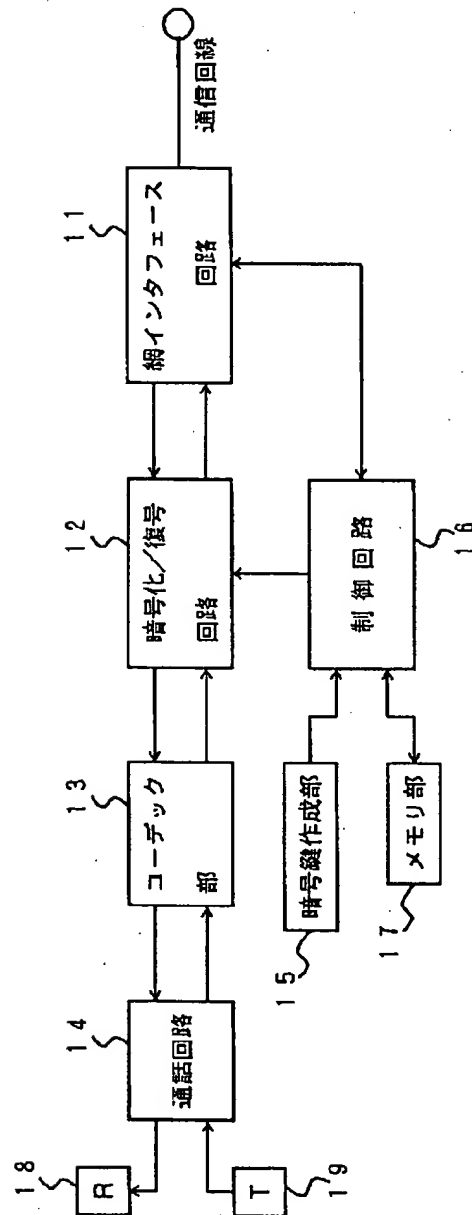
K_s : 通信用暗号鍵

K_i, K_j : 通信用暗号鍵解読鍵

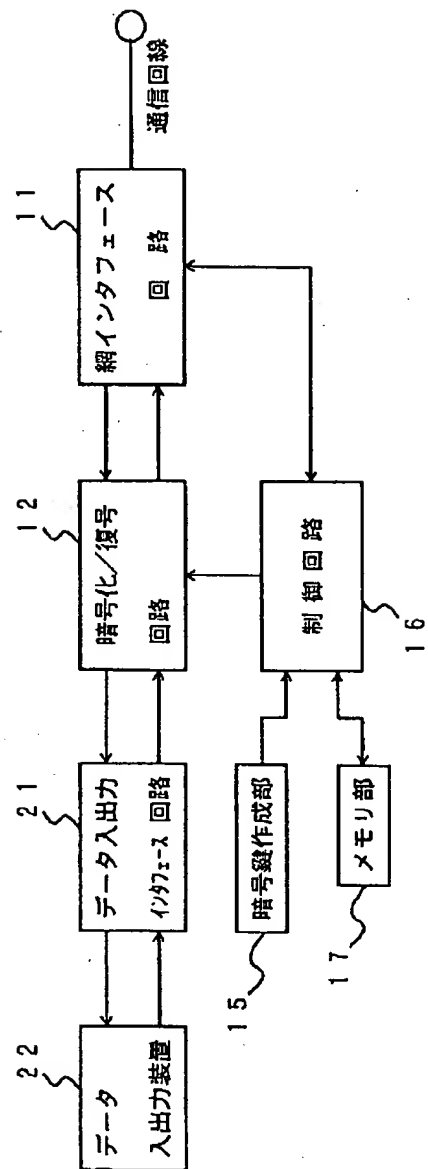
i, # j : 発信, 着信側ID



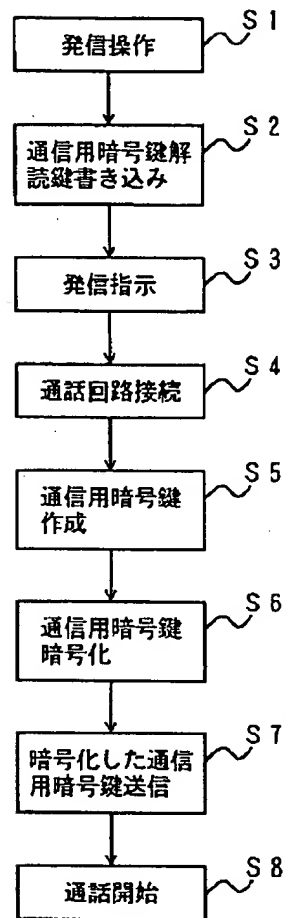
【図1】



【図5】



【図3】



【図4】

